EXHIBIT A

KEKER & VAN NEST LLP
ROBERT A. VAN NEST - # 84065
BRIAN L. FERRALL - # 160847
DAVID SILBERT - # 173128
MICHAEL S. KWUN - #198945
633 Battery Street
San Francisco, CA 94111-1809
Telephone: (415) 391-5400
Email: rvannest@kvn.com; bferrall@kvn.com; dsilbert@kvn.com; mkwun@kvn.com

SUSAN CREIGHTON, SBN 135528
SCOTT A. SHER, SBN 190053
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1700 K Street NW, Fifth Floor
Washington, D.C., 20006-3817
Telephone: (202) 973-8800
Email: screighton@wsgr.com; ssher@wsgr.com

JONATHAN M. JACOBSON, NY SBN 1350495
CHUL PAK (*pro hac vice*)
DAVID H. REICHENBERG (*pro hac vice*)
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1301 Avenue Of The Americas, 40th Floor
New York, NY 10019-6022
Telephone: (212) 999-5800
Email: jjacobson@wsgr.com; cpak@wsgr.com; dreichenberg@wsgr.com

Attorneys for Defendant ARISTA NETWORKS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

CISCO SYSTEMS, INC.,

Plaintiff,

v.

ARISTA NETWORKS, INC.,

Defendant.

Case No. 5:14-cv-05344-BLF (NC)

ARISTA'S [SAMPLE PROPOSED ORDER] RE ANALYTIC DISSECTION OF ASSERTED WORKS

Dept: Courtroom 3 - 5th Floor
Judge: Hon. Beth Labson Freeman

Date Filed: December 5, 2014

Trial Date: November 21, 2016

The Court has considered the briefing and evidence submitted by the parties in support of their respective positions regarding "analytic dissection" of the works asserted by Cisco, including declarations [and testimony] by the parties' experts, Dr. John Black and Dr. Kevin Almeroth. The Court has focused its analytic dissection on those aspects or features of the Cisco works that Cisco claims Arista has copied (the "Asserted Features"), recognizing that there are numerous other aspects of those works that may include both protectable and unprotectable elements. In performing analytic dissection, the Court has considered originality, the words-and-short-phrases doctrine, the idea/expression dichotomy (17 U.S.C. §102(b)), and the *scenes a faire* doctrine.

After consideration of the parties' arguments and evidence, the Court holds that a number of elements of the Asserted Features are not protectable under copyright law. The Court has not made the converse finding. That is, if elements of the Asserted Features are not listed below, that does not mean that the Court has found that they satisfy the requirements of originality or are not *scenes a faire*, or decided any other factual question underlying Cisco's infringement claim.

The following example further explains the Court's reasoning. The Border Gateway Protocol is a network routing protocol originally specified in June 1989 in Internet Engineering Task Force ("IETF") RFC No. 1105. RFC 1105 uses the acronym "BGP" to describe the protocol, and this acronym was part of the standard parlance in the networking industry before Cisco claims to have authored the asserted command-line-interface ("CLI") commands that use the term "BGP". The Court finds that the use of the term "BGP" in CLI commands relating to the BGP protocol is not protectable under copyright law. As a result, Cisco may not argue to the jury, and the jury may not find, that Arista's use of the term "BGP" itself supports a finding of infringement. Cisco is not precluded from arguing that other aspects of commands using the term BGP are protectable, subject to the evidence and any further rulings the Court may make before or during trial. Similar logic applies to the entirety of the Court's rulings herein.

The Court will instruct the jury that Arista's use of these elements, by itself, cannot support a finding of copyright infringement. The elements of the Asserted Features that the Court holds are not protectable are:

1. 198 CLI commands set forth in **Appendix A** hereto, which do not merit any presumption of originality and for which Cisco has offered no evidence, or no relevant evidence, carrying its burden that the phrases are original to Cisco (Unoriginality; *see* ECF No. 329 (Arista MSJ) at 8–10; ECF No. 329-15);
2. Acronyms, the names of protocols, and terms identifying standard networking features, functionality, and/or parameters that originate from formal or informal industry standards or widely-adopted conventions, which Cisco used in the Asserted Features consistently with pre-existing industry usage [sample set forth in **Appendix B]** (Unoriginality; *Scenes a faire*; *see* ECF No. 380 (Arista Opp. MSJ) at 9–11);
3. The hierarchical arrangement of Cisco commands by common root word, or sub-hierarchical arrangement by common first and second words, etc. (Section 102(b); Unoriginality; Words and short phrases (37 C.F.R § 202.1(a)); *Scenes a faire*; *see* ECF No. 329 (Arista MSJ) at 11–16);
4. The names of the asserted Cisco modes (EXEC, Privileged EXEC, Global Configuration and Privileged Configuration modes), their associated prompts, and the selection of commands that are available in each mode (Section 102(b); Unoriginality; *Scenes a faire*; Words and short phrases (37 C.F.R § 202.1(a)); *see* ECF No. 329 (Arista MSJ) at 11–17);
5. Functional elements of responsive screen displays, and elements of responsive screen displays taken from widely used industry conventions [sample set forth in **Appendix C]** (Section 102(b); Unoriginality; Words and short phrases (37 C.F.R § 202.1(a)); *Scenes a faire*);
6. To the extent Cisco asserts them as independently protectable under copyright, phrases of two words or fewer (Words and short phrases (37 C.F.R § 202.1(a)));
7. The command syntax in the form "[verb] [object or entity] [additional parameters]," which was used in pre-existing command languages and is not original to Cisco (Unoriginality; *Scenes a faire*);
8. The following command words, which were used in pre-existing command languages

and are not original to Cisco: "banner", "boot", "clock", "clear", "enable", "erase", "load", "set", "show" and "terminal" (Unoriginality, *Scenes a faire*);

9. The function of any Asserted Feature, such as the function of a particular command, or a mode of operation, or a command response screen (Section 102(b));

10. The use of a text-based command-line interface or CLI as opposed to another means of configuring or managing a device such as a graphical user interface, in which command words and arguments are typed in at a command prompt, and the use of multi-word commands to manage or configure a device (Unoriginality; Section 102(b)).

SO ORDERED.

_____, 2016

_____
HON. BETH LABSON FREEMAN
United States District Judge

Appendix A

1.	aaa accounting	51.	ip ospf authentication-key
2.	aaa accounting dot1x	52.	ip ospf cost
3.	aaa authentication login	53.	ip ospf dead-interval
4.	aaa authentication config-commands	54.	ip ospf hello-interval
5.	aggregate-address	55.	ip ospf network
6.	area default-cost	56.	ip ospf priority
7.	area default-cost (OSPFv3)	57.	ip ospf retransmit-interval
8.	area nssa	58.	ip ospf shutdown
9.	area nssa (OSPFv3)	59.	ip ospf transmit-delay
10.	area nssa default-information- originate	60.	ip pim anycast-rp
11.	area nssa default-information-originate (OSPFv3)	61.	ip pim log-neighbor-changes
12.	area nssa no-summary	62.	ip pim query-interval
13.	area nssa translate type7 always (OSPFv3)	63.	ip pim rp-address
14.	area range	64.	ip pim sparse-mode
15.	area range (OSPFv3)	65.	ip pim spt-threshold
16.	area stub	66.	ip pim spt-threshold group-list
17.	area stub (OSPFv3)	67.	ip tacacs source-interface
18.	bgp client-to-client reflection	68.	ip-community-list standard
19.	bgp cluster-id	69.	ipv6 access-group
20.	bgp confederation identifier	70.	ipv6 nd ra interval
21.	bgp confederation peers	71.	ipv6 nd ra lifetime
22.	bgp listen limit	72.	ipv6 nd ra suppress
23.	class-map type control-plane	73.	ipv6 nd router-preference
24.	clear counters	74.	isis hello-interval
25.	clear ip igmp group	75.	isis hello-multiplier
26.	clear ip mroute	76.	isis lsp-interval
27.	clear ip nat translation	77.	isis metric
28.	clear ip ospf neighbor	78.	isis passive
29.	clear spanning-tree counters	79.	isis priority
30.	clock set	80.	is-type
31.	clock timezone	81.	lacp rate
32.	default-metric (OSPF)	82.	load-interval
33.	dot1x timeout reauth-period	83.	log-adjacency-changes (IS-IS)
34.	enable secret	84.	logging host
35.	erase startup config	85.	mac access-group
36.	ip as-path access-list	86.	mac access-list
37.	ip community-list expanded	87.	neighbor activate
38.	ip community-list standard	88.	neighbor default-originate
39.	ip igmp query-interval	89.	neighbor ebgp-multihop
40.	ip igmp query-max-response-time	90.	neighbor fall-over bfd
41.	ip igmp startup-query-count	91.	neighbor next-hop-self
42.	ip igmp startup-query-interval	92.	neighbor remote-as
43.	ip igmp static-group	93.	neighbor remove-private-as
44.	ip igmp version	94.	neighbor route-map
45.	ip msdp group-limit	95.	neighbor send-community
46.	ip multicast boundary	96.	neighbor soft-reconfiguration
47.	ip multicast-routing	97.	neighbor update-source
48.	ip nat pool	98.	neighbor weight
49.	ip nat translation tcp-timeout	99.	network area
50.	ip nat translation udp-timeout	100.	ntp authenticate

101.	ntp authenticiation-key	151.	show isis database
102.	ntp server	152.	show isis interface
103.	ntp source	153.	show lacp counters
104.	ntp trusted-key	154.	show lacp interface
105.	policy-map type control-plane	155.	show lacp neighbor
106.	policy-map type pos	156.	show mac access-lists
107.	port-channel min-links	157.	show ntp associations
108.	radius-server deadtime	158.	show ntp status
109.	radius-server host	159.	show port-channel summary
110.	radius-server key	160.	show port-channel traffic
111.	radius-server retransmit	161.	show privilege
112.	radius-server timeout	162.	show radius
113.	routep-map	163.	show reload
114.	router isis	164.	show role
115.	router ospf	165.	show route-map
116.	routing-context vrf	166.	show snmp
117.	set-overload-bit	167.	show snmp chassis
118.	show clock	168.	show snmp community
119.	show dot1x statistics	169.	show snmp contact
120.	show environment power	170.	show snmp location
121.	show interfaces switchport backup	171.	show snmp source-interface
122.	show ip bgp community	172.	show snmp trap
123.	show ip bgp neighbors	173.	show spanning-tree blockedports
124.	show ip bgp paths	174.	show spanning-tree bridge
125.	show ip bgp regexp	175.	show spanning-tree interface
126.	show ip bgp summary	176.	show spanning-tree mst configuration
127.	show ip igmp groups	177.	show spanning-tree mst interface
128.	show ip igmp interface	178.	show spanning-tree root
129.	show ip igmp snooping groups	179.	show tacacs
130.	show ip igmp snooping querier	180.	show user-account
131.	show ip mfib	181.	show version
132.	show ip mroute	182.	show vlan summary
133.	show ip mroute count	183.	show vrf
134.	show ip msdp mesh-group	184.	snmp trap link-status
135.	show ip nat translations	185.	snmp-server chassis-id
136.	show ip ospf	186.	snmp-server contact
137.	show ip ospf border-routers	187.	snmp-server enable traps
138.	show ip ospf database database-summary	188.	snmp-server location
139.	show ip ospf interface	189.	snmp-server view
140.	show ip ospf neighbor	190.	spanning-tree bridge assurance
141.	show ip ospf request-list	191.	spanning-tree transmit hold-count
142.	show ip ospf retransmission-list	192.	spf-interval
143.	show ip pim interface	193.	statistics per-entry
144.	show ip pim neighbor	194.	switchport backup interface
145.	show ip pim rp	195.	tacacs-server key
146.	show ip route summary	196.	username sshkey
147.	show ipv6 bgp	197.	vrf definition
148.	show ipv6 bgp community	198.	vrf forwarding
149.	show ipv6 bgp neighbors		
150.	show ipv6 bgp summary		

Appendix B

[Examples of unoriginal acronyms and keywords that comprise the Asserted Features. Within each family, the listed root word (e.g., "aaa") as well as combinations of that root word with the terms that follow it are all unprotectable]

1. Aaa
    a. Accounting
        i. Dot1x
    b. Authentication
        i. login
    c. Authorization
    d. Server
        i. Radius
        ii. Tacacs+

* * *

2. Bgp
    a. Reflection
    b. Cluster id
    c. Confederation
        i. Identifier
        ii. Peers

* * *

Appendix C

[Examples of unoriginal acronyms and keywords used in the accused command responses]

1. The following unoriginal acronyms and keywords that appear in the command response to the CLI command "show ip route" are unprotectable:
    a. route
    b. static
    c. aggregate
    d. RIP
    e. BGP
    f. OSPF
    g. NSSA
    h. IS-IS
2. The following unoriginal acronyms and keywords that appear in the command response to the CLI command "show snmp" are unprotectable:
    a. SNMP
    b. community name
    c. trap
3. The following unoriginal acronyms and keywords that appear in the command response to the CLI command "show interface ethernet" are unprotectable:
    a. Ethernet
    b. address
4. The following unoriginal acronyms and keywords that appear in the command response to the CLI command "show ip igmp snooping" are unprotectable:
    a. IGMP
    b. snooping